Gartner Research

Augmented Cybersecurity: Act Now to Thrive Amid Chaos and Complexity

Cybersecurity Research Team

29 May 2024

Gartner®

Augmented Cybersecurity: Act Now to Thrive Amid Chaos and Complexity

29 May 2024 - ID G00816719 - 13 min read

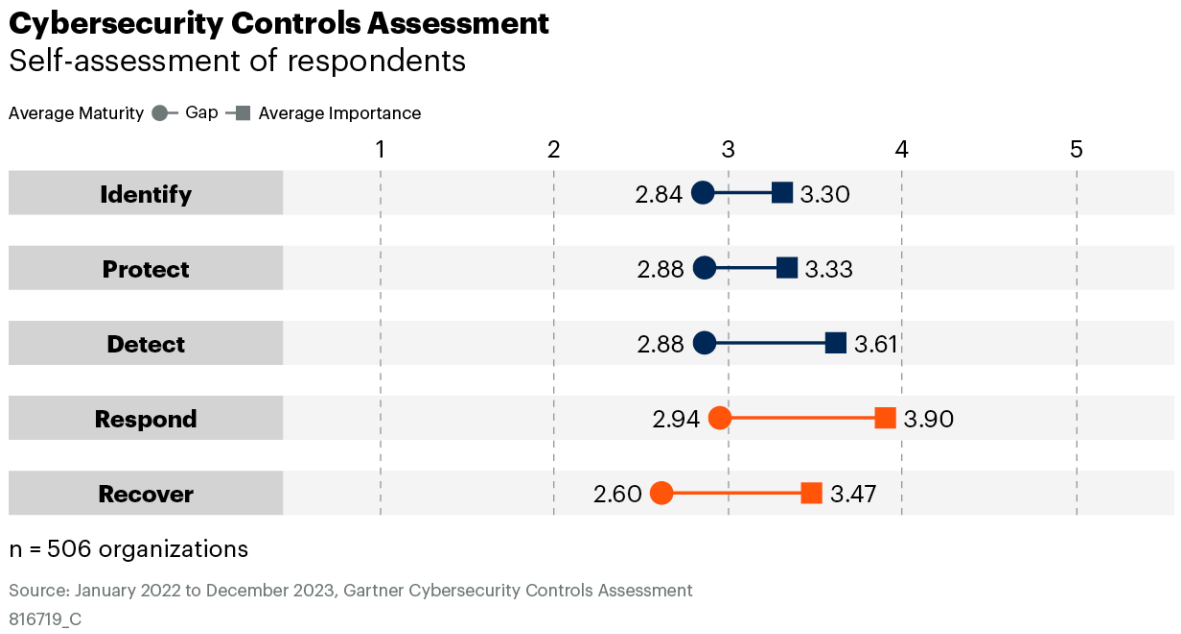
By Analyst(s): Cybersecurity Research Team

Initiatives: Cyber Risk; Build and Optimize Cybersecurity Programs

> "Zero tolerance for failure" mindsets must be abandoned for organizations to thrive in increasingly complex environments. Augmented cybersecurity delivers sustainable cybersecurity outcomes by elevating response and recovery to an equal status with prevention.

This mindset is evident in both cybersecurity's outsized preoccupation with preventing potential attacks and its collective underinvestment in fixing the damage that attacks might cause. While cybersecurity leaders rank "respond" and "recover" as more important than "protect," Gartner's Cybersecurity Controls Assessment reveals that when it comes to maturity, response and recovery have the largest gaps between current and desired states (see Figure 1).

Figure 1: Cybersecurity Controls Assessment



A cybersecurity strategy that disproportionately focuses on prevention of security incidents is unsustainable and does not yield results for the organization or for the cybersecurity team.

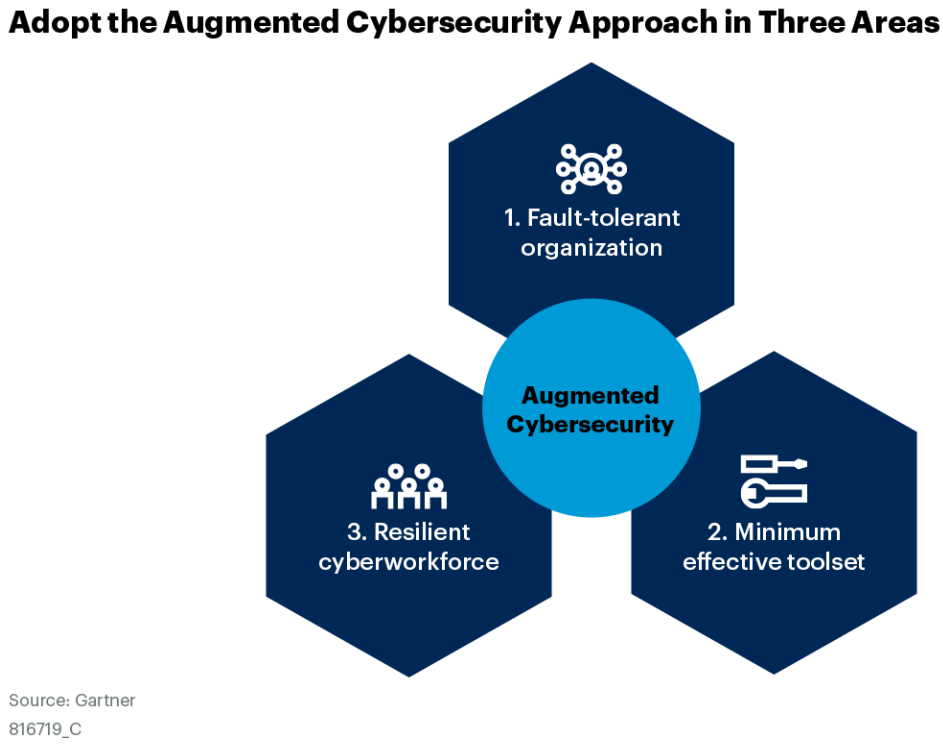
To thrive and not just survive in a complex operating environment, cybersecurity leaders need to adopt an "augmented cybersecurity" approach. This approach sustainably defends the organization by elevating response and recovery to equal status with prevention. Gartner recommends cybersecurity leaders start adopting this approach in three areas (see Figure 2):

1. **Build a fault-tolerant organization:** How does your organization use generative AI (GenAI) and engage with third parties?

2. **Embrace a "minimum effective toolset" approach:** How do you manage cybersecurity's technology portfolio?

3. **Develop a resilient cyberworkforce:** How do you manage and lead the cybersecurity team?

Figure 2: Augmented Cybersecurity



Build a Fault-Tolerant Organization

Security leaders should start elevating response and recovery to the same level as protection in two of the areas where risk exposures are continuously increasing — the way organizations use GenAI and how they engage with third parties.

They must formulate response and recovery plans for GenAI by asking:

1. If our data is not AI-ready, how much hallucination is tolerable?
2. What alternatives to AI are available to achieve the objective?
3. What is the cost of switching to another approach if we need to?
4. Can we “pull the plug” if something goes wrong?

Similarly, security leaders should bring business continuity management practices to third-party cyber risk management (TPCRM) by:

- Creating a formal third-party contingency plan (include an exit strategy plan, alternative suppliers list and incident response playbooks).
- Conducting third-party incident response exercises.
- Working with third parties to mature their security risk management practices as necessary.

Each of these three actions improves TPCRM effectiveness by more than 40%. [1]

Embrace a "Minimum Effective Toolset" Approach

Security leaders typically overinvest in prevention tools and controls. This investment isn't yielding the desired results as cybersecurity incidents continue to rise. At the same time, understrength security teams find it harder to manage the confusing array of security technology point solutions.

Cybersecurity leaders should map their tools to their controls framework to identify capability gaps and redundancies. They should also strive to consolidate multiple stand-alone cybersecurity products into platforms to improve their risk posture and efficiency. Sixty-five percent of participants in the 2022 Gartner CISO: Security Vendor Consolidation XDR and SASE Trends Survey said that the primary benefit of security vendor consolidation is improvement in overall organizational risk posture. [2]

Security leaders should ask themselves: "What is the minimum number of tools required to effectively observe, defend and respond to exploitations of the organization's exposures?"

To get the most out of new technology investments, cybersecurity leaders should learn about the proven enterprise value and deployment risks of different technologies. Review Gartner's Infographic: 2024 Technology Adoption Roadmap for Security and Risk Management to understand the different security-related technologies being adopted by global enterprises, and compare your technology investments with those of your peers.

Gartner predicts that, by 2026, AI will increase SOC efficiency by 40% compared to 2024, beginning a shift in SOC expertise toward AI development, maintenance and protection. [3] Security leaders must aggressively pursue GenAI-driven efficiencies and explore GenAI augments within the cybersecurity function.

Develop a Resilient Cyberworkforce

Sixty-two percent of cybersecurity leaders have experienced burnout at least once in the past year. [4] One of the causes of this burnout is the "zero tolerance for failure" mindset of cybersecurity professionals that pushes them to completely focus on *preventing* a bad outcome, even if it comes at the cost of their personal health and well-being. And if they don't succeed in that mission, they try to hide their failures and continue to operate under great stress, which only compounds the problem.

To develop resilience as a core cybersecurity workforce competency (rather than a trait we assume everyone has) cybersecurity leaders need to do three things:

1. Prioritize employee well-being even during active incident response by grouping more experienced analysts with less experienced ones, building counseling and stress-relief activities into incident workflows, and augmenting teams with external partners where needed.

2. Build a culture that encourages experimentation and views mistakes as learning opportunities. Examples of this include creating a new metric: "Days since last learning opportunity," and creating a system of rewards and recognition for praiseworthy failures.

3. Redesign workflows by actively seeking employee feedback on bottlenecks,reducing process friction, and making processes adaptable.

This resource contains the actions you need to drive the adoption of an augmented cybersecurity approach. We have carefully selected Gartner research to help your organization thrive and not just survive in an increasingly complex business and technology environment.

Analysis

Cybersecurity professionals are stuck in "survival" mode. This is not because of the vast number of threat actors, the ever-expanding attack surfaces or the chronic shortage of cybersecurity talent. What stops them from thriving amid chaos and complexity is the mindset of zero tolerance for failure that continues to pervade cybersecurity and organizational cultures.

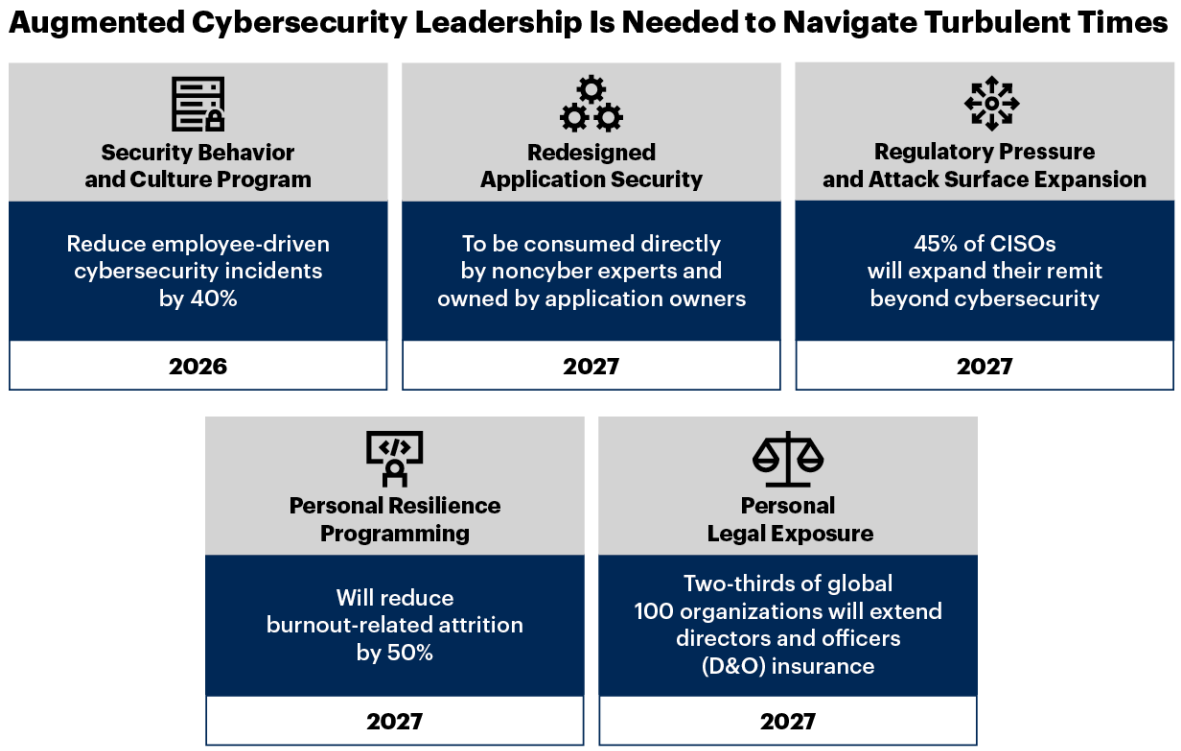
Why Augmented Cybersecurity Leadership Is Essential

Augmented cybersecurity leadership ties human talent to technology capabilities and balances organizational growth aspirations and cyber risk. It invests in personal resilience programming to reduce employee burnout specifically in the cybersecurity workforce. Augmented cybersecurity helps navigate a complex operating environment by making resilience a conscious choice, not an adrenaline-fueled exercise.

- Maverick* Research: You Will Be Hacked, So Embrace the Breach: Cybersecurity breaches are inevitable, but many security and risk management leaders still think they can prevent all hacks by throwing people and money at their defenses. Instead of striving so hard to prevent breaches, understand how to build resilience and learn from security incidents.

- Predicts 2024: Augmented Cybersecurity Leadership Is Needed to Navigate Turbulent Times: Review this research to learn why security and risk management leaders of the future need to be AI-enabled, human-centric decision makers to effectively steer through turbulent times (see Figure 3).

Figure 3: Augmented Cybersecurity Leadership Is Needed to Navigate Turbulent Times



Build a Fault-Tolerant Organization

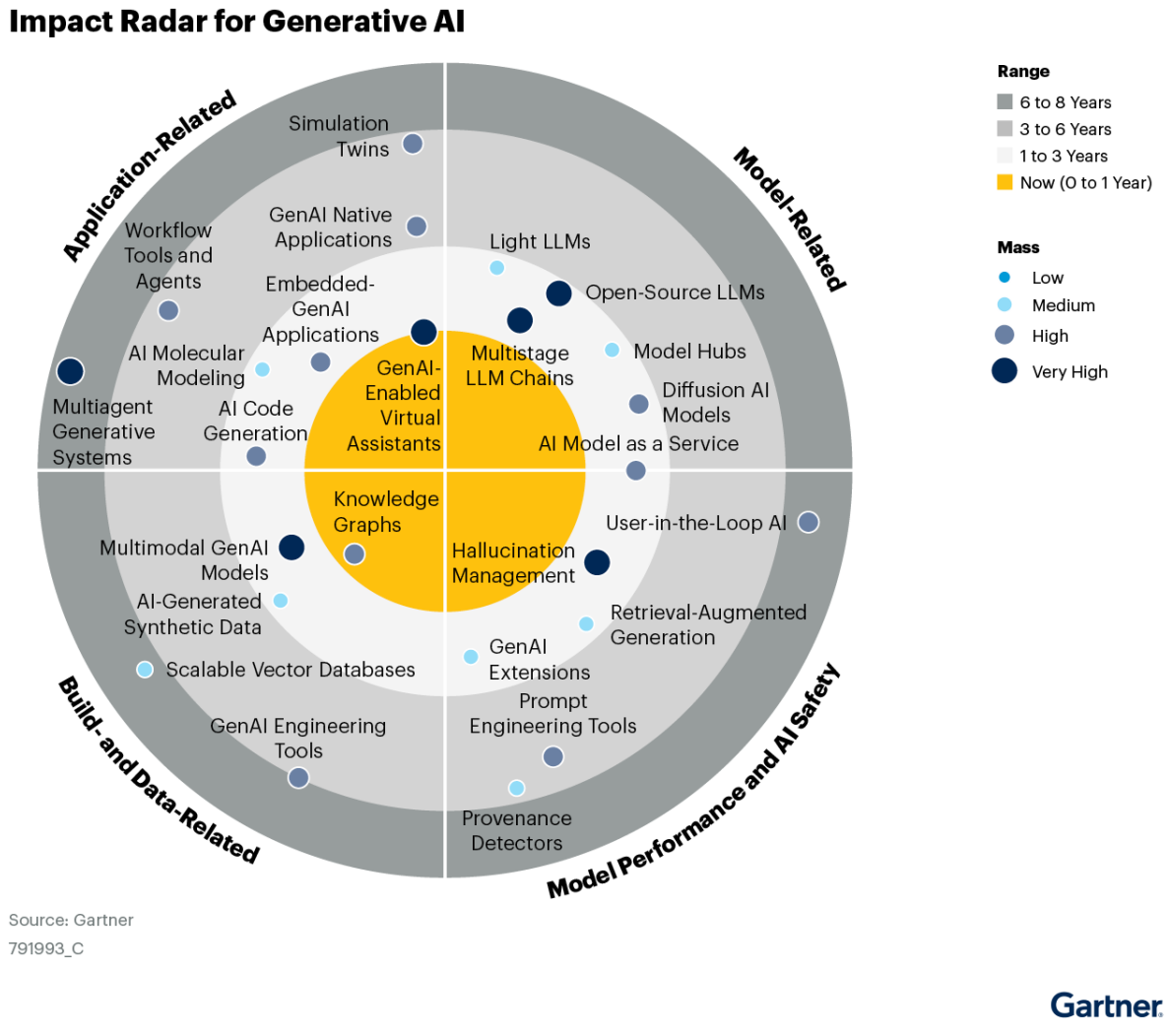
Build Response and Recovery Plans for Generative AI Use Cases

For a rapidly evolving technology like GenAI, it is impossible to prevent every security incident. Therefore, your ability to adapt, respond, and recover effectively from inevitable issues, whether internal/external or malicious/inadvertent, is critical to enable your organization to explore GenAI successfully.

The following resources contain recommendations and tools to help you build response and recovery plans for GenAI use at your organization.

- Emerging Tech Impact Radar: Generative AI: An analysis of the maturity, market momentum, and influence of GenAI-related emerging technologies and trends. Learn the key components that you must understand to exploit GenAI opportunities and securely deliver value (see Figure 4).

Figure 4: Impact Radar for Generative AI



Source: Gartner
791993_C

Gartner

- Predicts 2024: AI & Cybersecurity — Turning Disruption Into an Opportunity: Learn how security and risk management leaders can prepare for GenAI evolution and progressively integrate GenAI features to augment their security workflows.
- Tool: Generative AI Security Policy Template: This tool provides a starting point for defining GenAI security governance. Organizations planning to leverage or currently leveraging GenAI should use this template to define, document, and publish clear guidelines for secure development and use of GenAI capabilities, tools and services.
- Tool: Roadmap for Deploying and Managing Generative AI: Organizations need to coordinate activities for GenAI to support agility. Use this roadmap template and guidance to plan and sequence activities in delivering GenAI projects.

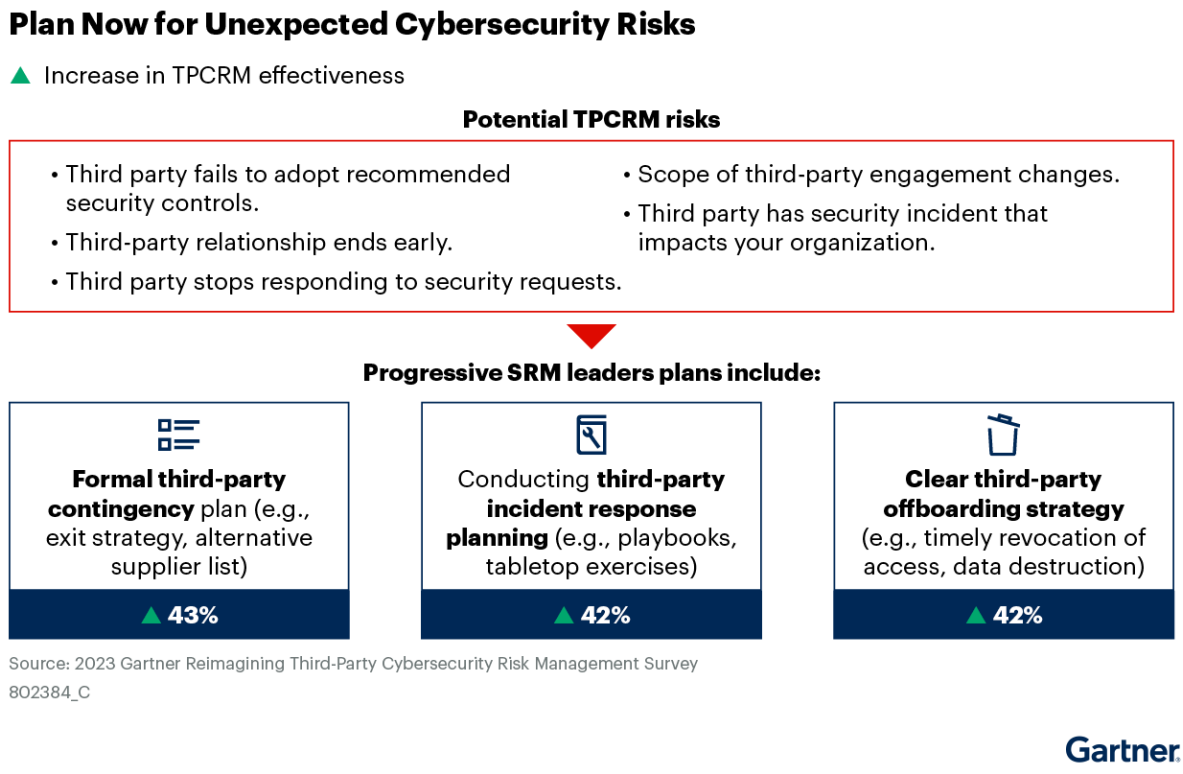
Upgrade Response and Recovery Plans for Third-Party Engagements

Conducting incident response planning (playbooks, tabletop exercises, etc.) and having a formal third-party contingency plan (e.g., exit strategy, alternative supplier list) increases TPCRM effectiveness by 42% and 43%, respectively. [1]

The following resources contain recommendations and tools to help you build response and recovery plans for your organization's third-party engagements:

- Infographic: Minimize Disruption From Third-Party Cybersecurity Risks: TPCRM is often resource-intensive, overly process-oriented and has little to show for in terms of results. Review this research to learn the actions successful CISOs take to improve their approach to TPCRM.
- 4 Ways to Boost Third-Party Cybersecurity Risk Management Effectiveness: Review this research to learn how to manage third-party cybersecurity risks in a scalable and resilience-focused manner (see Figure 5).

Figure 5: Plan Now for Unexpected Cybersecurity Risks



- Podcast: Wrangling Third-Party Cyber Risk Management: Listen to this podcast to learn how to make contingency planning a core element of TPCRM.

- CISOs: 3 Steps to Business Accountability for Third-Party Cybersecurity Risks: Learn how the Cybersecurity team at RWE, a German multinational energy company, promoted business accountability of third-party cybersecurity risks throughout the third-party life cycle.

Embrace a “Minimum Effective Toolset” Approach

Identify Redundancies and Gaps by Mapping Your Toolset to Your Controls Framework

Cybersecurity leaders and their teams can struggle with the complexity, overlap and blind spots that arise from using a large number of disparate cybersecurity tools.

The following resources contain recommendations and tools to help you adopt a minimum effective toolset approach:

- Infographic: Map Your Cybersecurity Controls Performance and Investments: Use this infographic to identify gaps between maturity and importance as mapped to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and what’s driving the lowest-performing controls categories.
- Cybersecurity Controls Assessment: This assessment tool offers a self-assessed view of controls implementation maturity against leading industry-recognized frameworks and standards. It enables cybersecurity leaders to conduct peer benchmarking relevant to their industry and level of risk exposure.
- Tool: Cybersecurity Platform Consolidation Workbook: Consolidating multiple stand-alone cybersecurity products into platforms, whenever appropriate, helps organizations improve their risk posture and their efficiencies. Use this tool to structure your approach to assessing and deciding on cybersecurity consolidation projects.

Build Effective Technology POCs That Focus on Frequent Deployment Risks

Build your new technology evaluation plans by focusing on the four frequent deployment risks identified by your peers — cybersecurity risks, talent unavailability, high or unpredictable costs, and technical incompatibility.

The following resources contain recommendations and tools to help you build effective technology proofs of concept (POCs):

- Infographic: 2024 Technology Adoption Roadmap for Security and Risk Management: This Infographic identifies 44 security-related technologies being adopted by global enterprises, and maps them according to adoption phase, deployment risk and enterprise value. Use this Infographic to compare your technology investments with those of your peers.
- Emerging Tech Impact Radar: Security: Incorporate the emerging technologies and services outlined in this research to expand growth opportunities linked to organizations' need to proactively mitigate exposure, effectively detect and respond to attacks, and create better efficiencies through AI-based security hyperautomation.

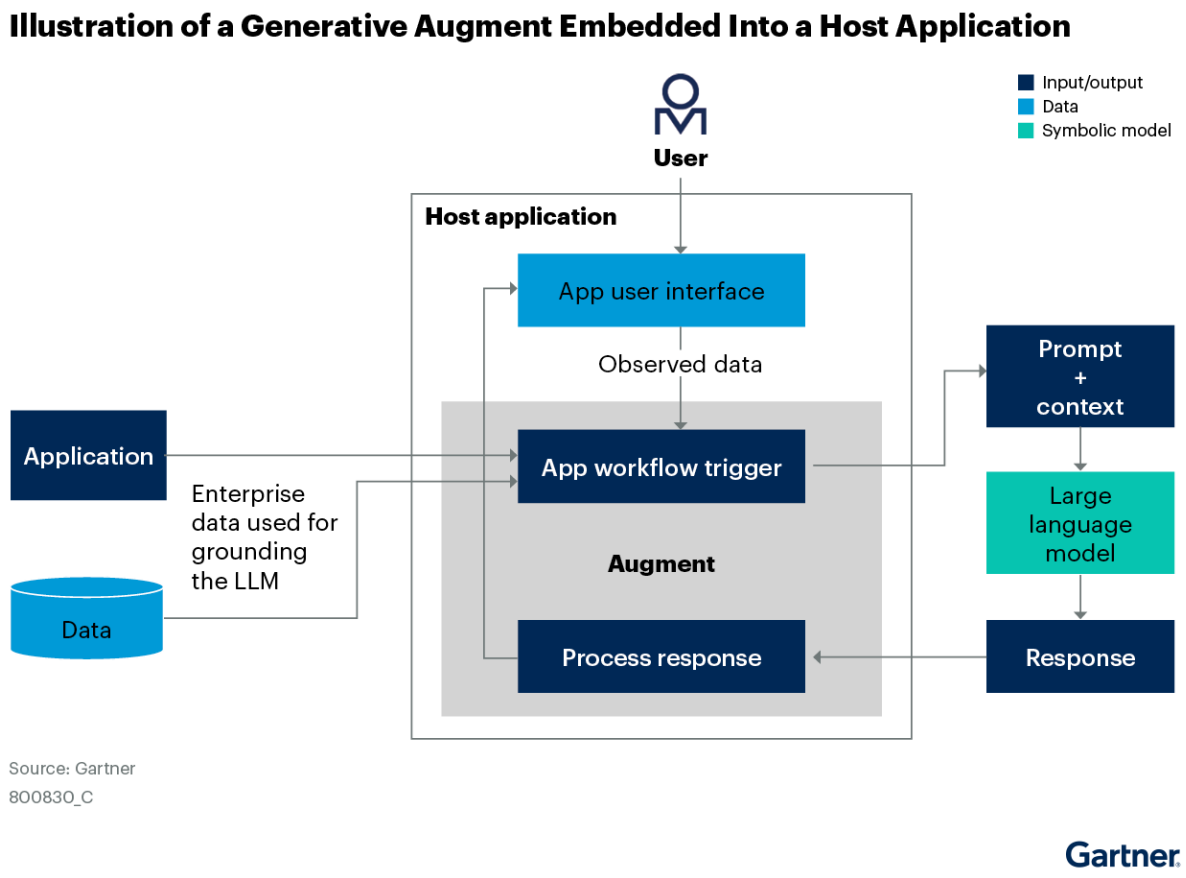
Aggressively Pursue GenAI-Driven Efficiencies and Explore GenAI Augments

Gartner predicts that, by 2026, AI will increase SOC efficiency by 40% compared to 2024, beginning a shift in SOC expertise toward AI development, maintenance and protection. [3]

The following resources contain recommendations and tools to help you improve your teams' capabilities by adopting Gen-AI:

- How CISOs Are Supercharging Their Teams With Generative AI Augments: Generative AI augments are purpose-built to improve knowledge-worker productivity, address the cybersecurity skills shortage, and mitigate risks from large language models. Review this research to learn how to improve your teams' capabilities by adopting generative augments (see Figure 6).

Figure 6: Illustration of a Generative Augment Embedded Into a Host Application



- Identity and Access Intelligence Innovation With Generative AI: GenAI provides opportunities and threats that will transform identity and access management (IAM) operating models. Use this research to understand use cases and develop an architecture strategy to safely adopt GenAI in IAM.

Develop a Resilient Cyberworkforce

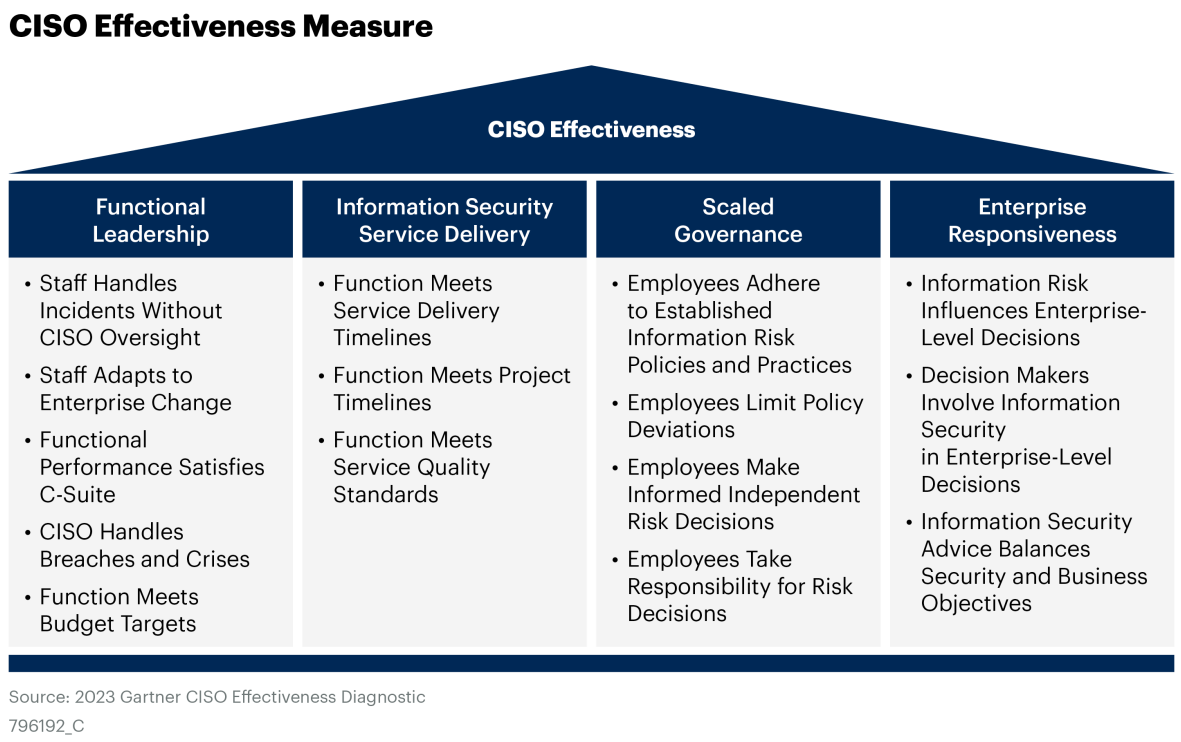
Treat Personal Resilience as a Professional Competency and Build It Into Workflows

Cybersecurity is suffering from a mental health crisis. Many cybersecurity professionals at all levels are struggling with the seemingly impossible mandate to protect the organization — amid growing threats, resource constraints and insufficient executive support — and then demonstrate how they're delivering business value. Unmanaged, the current crisis will drive a vicious cycle of burnout, attrition and increased cyber risk.

The following resources contain recommendations on how to develop a resilient cyberworkforce and promote employee well-being:

- CIOs Must Adopt AI and Unconventional Talent to Create a Resilient IT Workforce: This research, which is based on the findings of the 2023 Gartner Resilient Workforce Model of the Future Survey, highlights what CIOs need to do to address talent shortages and build a more resilient workforce.
- CISO Effectiveness: Start Practicing 3 Burnout-Avoiding Behaviors Now: CISOs are burning out from decision, data and device overload. Use this research to address these three fatigue drivers at their source.
- CISO Effectiveness Diagnostic: Use this diagnostic to benchmark effectiveness in the CISO role and receive targeted recommendations to develop the four distinct categories of behaviors and mindsets that differentiate top cybersecurity leaders (see Figure 7).

Figure 7: CISO Effectiveness Measure



Source: 2023 Gartner CISO Effectiveness Diagnostic
796192_C

Gartner

Research Highlights

Some recommended content may not be available as part of your current Gartner subscription.

Contributors

Richard Addiscott, Ant Allan, Selena Granado-Kral, Mark Horvath, Akif Khan, Christine Lee, Chris Mixter, Pete Shoard, Andrew Walls, Dennis Xu.

Evidence

[1] **2023 Gartner Reimagining Third-Party Cybersecurity Risk Management Survey:** This research initiative involved surveying 376 senior executives involved in third-party cybersecurity risk management across organizations from different industries, geographies and sizes. This research was further substantiated and informed by in-depth practitioner interviews with over 60 chief information security officers (CISOs) to understand cybersecurity goals and challenges associated with third-party cybersecurity risk management. The survey was conducted from July through August 2023. The objective of the survey was to understand the practices that cybersecurity leaders should follow to better manage cybersecurity risks emanating from third-party relationships. Gartner used descriptive statistics to ensure all normal distribution of data and created a measure of effectiveness that determines how effective an organization is in achieving key cybersecurity outcomes. We then used a regression-based maximum impact analysis to determine which of the hypothesized practices in third-party cybersecurity risk management were most impactful in improving those outcomes. Maximum impact shows the largest amount of improvement in outcomes that an organization can realize by improving each factor in managing third-party cybersecurity risk. *Disclaimer: Results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.*

[2] **2022 Gartner CISO: Security Vendor Consolidation XDR and SASE Trends Survey:** This study was conducted to determine how many organizations are pursuing vendor consolidation efforts, what the primary drivers are for consolidation, expected or realized benefits of vendor consolidation, and how those who are consolidating are prioritizing their consolidation efforts. The primary purpose of this survey was to collect objective data on extended detection and response (XDR) and secure access service edge (SASE) for consolidation of megatrend analysis. The research was conducted online during March and April 2022 among 418 respondents from North America (U.S., Canada), Asia/Pacific (Australia, Singapore) and EMEA (France, Germany, U.K.). Results were from respondents with $50 million or more in 2021 enterprisewide annual revenue. Industries surveyed included manufacturing, communications and media, information technology, government, education, retail, wholesale trade, banking and financial services, insurance, healthcare providers, services, transportation, utilities, natural resources, and pharmaceuticals, biotechnology and life sciences. Respondents were screened for job title, company size, job responsibilities to include information security/cybersecurity and IT roles, and primary involvement in information security. *Disclaimer: Results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.*

[3] Predicts 2024: AI & Cybersecurity — Turning Disruption Into an Opportunity.

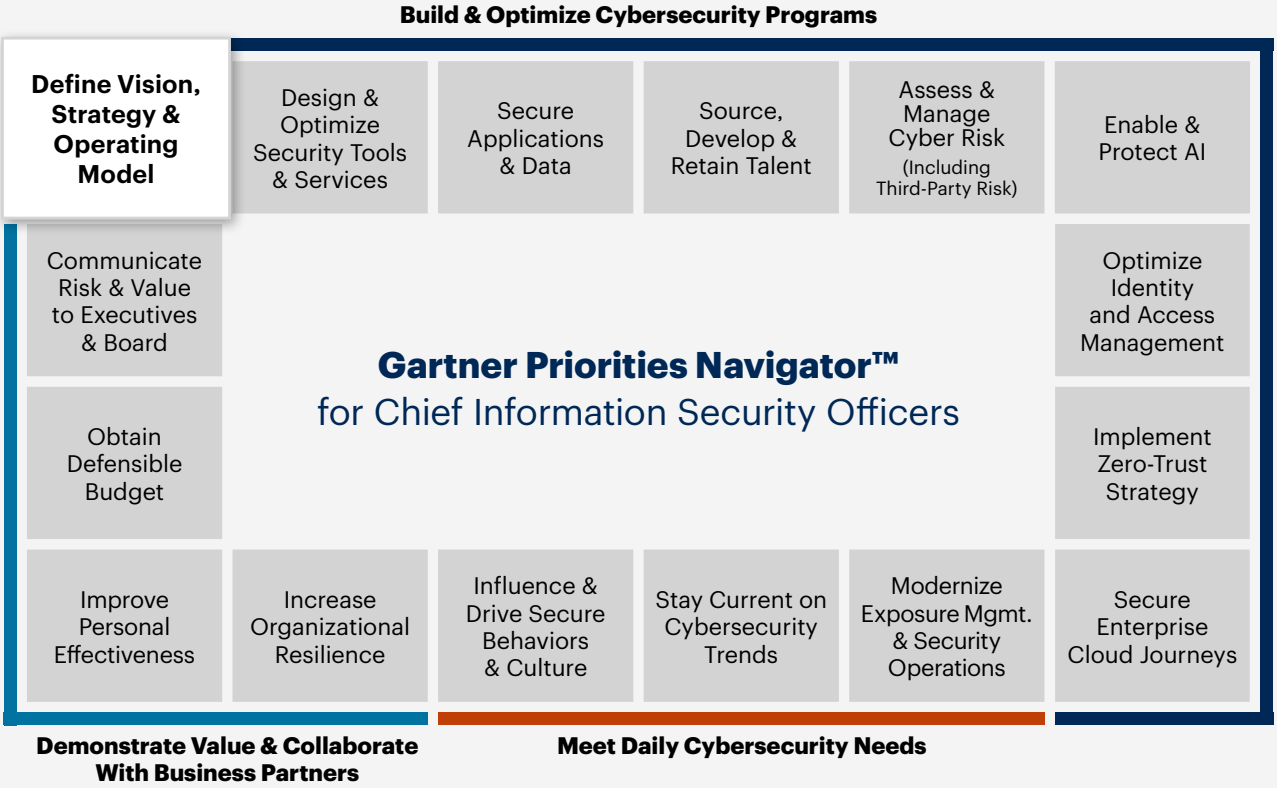
[4] Cybersecurity Leaders Are Burned Out. Here's Why.

Gartner Priorities Navigator™ for CISOs

Build & Optimize Cybersecurity Programs

The Gartner Priorities Navigator™ represents critical areas where Gartner provides supportive expert advice and tools to CISOs and their teams.

This research is a part of the Gartner research focused on developing a strategy to source, develop and retain talent. Each of these priorities features further research and resources available to **Gartner for Chief Information Security Officer** clients.



By 2027, 45% of CISOs will expand their remit beyond cybersecurity, due to increasing regulatory pressure and attack surface expansion.

Source: Gartner

Questions your peers are asking Gartner

- How do I develop a coherent vision for our cybersecurity program?
- What are the elements of a cybersecurity strategy, and how do I develop them?
- How are security operating models changing in response to the democratization of IT?

How Gartner helps

Key Insights for the Chief Information Security Officer

Unique and exclusive insights to help CISOs and their teams succeed

Be a better leader
Cybersecurity leadership insights in key areas:

- Role, relationships, talent and culture
- Business value and strategy
- Cybersecurity program

Be a better business partner
Cross-functional insights including:

- Enterprise risk management
- Future of Work, Risk Response Strategies, Change management

Thrive with tech insights

- Trends on emerging tech advances
- Contextualized industry insights

Expert Guidance

Regularly connect with experts, who have been in cybersecurity leadership roles, who speak to a diverse set of leaders every day, and who truly understand the challenges you face and the insights that will help you fully achieve your goals.

Decisioning Tools

Tools to **turn strategy into action** by helping accelerate key initiatives and drive better business outcomes.

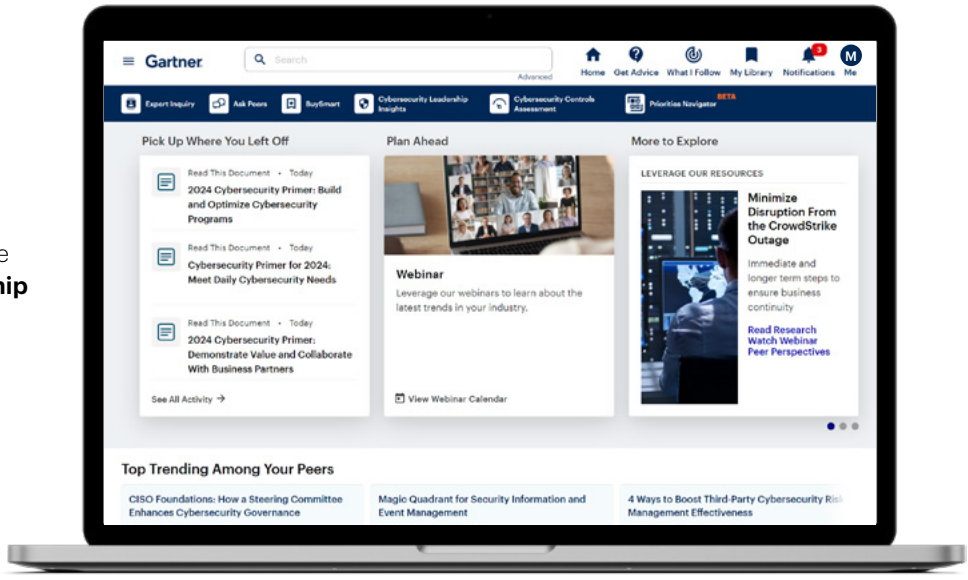
Peer Networks

One-on-one chats with other industry leaders, peer-led discussions, polls, and access to technology ratings and reviews.

Engaging Events

VIP access at Gartner Security & Risk Management Summit with numerous educational breakout sessions, and many more opportunities to connect with peers and Gartner experts. Plus, apply to be part of the CISO Circle for exclusive sessions and networking opportunities.

A customized gartner.com experience to ensure you're **optimizing your partnership with Gartner.**



Actionable, objective insight

Position your organization for success. Explore these additional complimentary resources and tools for cybersecurity leaders:

Report

Cybersecurity Trends: Optimize for Resilience and Performance

Use this report to equip your cybersecurity function for greater resilience.

Download Now

Roadmap

IT Roadmap for Cybersecurity

Create a resilient, scalable and agile cybersecurity strategy.

Download Now

eBook

Leadership Vision for Security and Risk Management Leaders

Explore the top 3 strategic priorities for SRM leaders.

Download Now

Webinar

Strengthen Your Cybersecurity Leadership to Navigate Evolving Security Landscape

Explore this 5-part series for insights into the evolving landscape.

Watch Now

Already a client?
Get access to even more resources in your client portal. Log In

Connect With Us

Get actionable, objective insight that drives smarter decisions and stronger performance on your mission-critical priorities. Contact us to become a client:

U.S.: 1 866 263 8917

International: +44 (0) 03301 628 476

Become a Client

Learn more about Gartner for Cybersecurity Leaders
gartner.com/en/cybersecurity

Stay connected to the latest insight

Gartner®